2015

# Quantum oblivious set-member decision protocol

Run-hua Shi
*University of Wollongong*, rshi@uow.edu.au

Yi Mu
*University of Wollongong*, ymu@uow.edu.au

Hong Zhong
*Anhui University*

Shun Zhang
*Anhui University*

## Publication Details

Shi, R., Mu, Y., Zhong, H. & Zhang, S. (2015). Quantum oblivious set-member decision protocol. Physical Review A: Atomic, Molecular and Optical Physics, 92 022309-1-022309-5.

# Quantum oblivious set-member decision protocol

**Abstract**
We present and define a privacy-preserving problem called the oblivious set-member decision problem, which allows a server to decide whether a private secret of a user is a member of his private set in an oblivious manner. Namely, if the secret belongs to his private set, he does not know which member it is. We propose a quantum solution to the oblivious set-member decision problem. Compared to classical solutions, the proposed quantum protocol achieves an exponential reduction in communication complexity, since it only needs $O(1)$ communication cost.

**Disciplines**
Engineering | Science and Technology Studies

**Publication Details**
Shi, R., Mu, Y., Zhong, H. & Zhang, S. (2015). Quantum oblivious set-member decision protocol. Physical Review A: Atomic, Molecular and Optical Physics, 92 022309-1-022309-5.

# Quantum Oblivious Set-Member Decision Protocol

Run-hua Shi[1,2] Yi Mu[2] Hong Zhong[1] Shun Zhang[1]

1. School of Computer Science and Technology, Anhui University, Hefei City, 230601, China
2. Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong NSW 2522, Australia

We present and define a new privacy-preserving problem, called Oblivious Set-member Decision problem, which allows a server to decide whether a private secret of a user is a member of his private set in an oblivious manner. Namely, if the secret belongs to his private set, he doesn't know which member it is. We propose a quantum solution to the Oblivious Set-member Decision problem. Compared to classical solutions, the proposed quantum protocol achieves an exponential reduction in communication complexity, since it only needs $O(1)$ communication cost.

**PACS numbers**: 03.67.Ac, 03.67.Dd, 03.67.Hk

## I. INTRODUCTION

The 21st century is the era of information. However, information brings us not only opportunities and fortunes but also problems and troubles, such as the overflow of junk information, the loss of important information and the leakage of privacy information. Especially, among these problems, how to protect privacy has become the focus of widely attentions these days.

Furthermore, with the rapid development of the technologies of quantum communication and quantum computation, researchers began to consider quantum methods to solve privacy-preserving problems, such as blind quantum computing [1-5], quantum homornorphic encryption [6], quantum private query [7-10], quantum bit commitment [11-14], quantum oblivious transfer [15-17] and so on.

In this paper, we consider a new but interesting privacy-preserving problem. Imagine that a user, Alice, has a private secret and a server, Bob, owns a private set. Bob wants to know whether Alice's private secret is a member of his private set, but Alice does not want him to know her secret (privacy) and further which member of his private set it is equal to (anonymity). In this paper, we call it Oblivious Set-member Decision (OSMD) problem. Obviously, OSMD can be used to privately compute the cardinality of set intersection and union. In addition, it is also widely applied in fields of the identifiable and verifiable circumstances as a primitive protocol. For example, suppose that there is a server and $n$ users ($U_1, U_2, \ldots, U_n$), who form a special distributed group (e.g., health system) via wire or wireless networks, and the server only provides resources or services for his authorized users. During the initialization phase, the server randomly generates a unique secret $k_i$ for every legal user $U_i$. During the Authentication phase, the user requests the server to execute an OSMD protocol, so that the server can decide whether the private secret of the user lies in the set, $K$, which consists of all authorized user's secrets generated by the server in advance. If $k_i \in K$ (but $i$ is unknown), then the user $U_i$ is an authorized user and further the server opens the corresponding resources or provides services to him/her. Otherwise, the verification fails. Obviously, it does not reveal any identity information of the user while executing the OSMD protocol; that is, it satisfies the request of the anonymous property.

Suppose that Alice has a secret, $k$, and Bob a private set, $\{k_1, k_2, \ldots, k_n\}$. In classical settings, in order to protect Alice's anonymity, it is necessary to make a decision of each $k \neq k_i$ by Alice and Bob collaboratively, not just by Bob independently. Since $k \notin \{k_1,k_2,\ldots,k_n\} \Leftrightarrow (k \neq k_1) \wedge (k \neq k_2) \wedge \ldots \wedge (k \neq k_n)$, it needs at least $O(n)$ communication costs to solve the OSMD problem in classical settings. In this paper, however, we propose a quantum OSMD protocol, which only needs $O(1)$ communication cost.

## II. THE PROTOCOL

### A. DEFINITION

We first define Oblivious Set-member Decision problem as follows.

**Definition 1** (Oblivious Set-member Decision Problem): Alice has a private secret, $k$, and Bob a private set, $\{k_1, k_2, \dots, k_n\}$. Bob wants to know whether Alice's secret $k$ belongs to the set of $\{k_1, k_2, \dots, k_n\}$ in an oblivious manner. That is, though Bob finally know whether $k$ is a member of the set of $\{k_1, k_2, \dots, k_n\}$, he doesn't know which member it is and further doesn't know Alice's secret $k$ yet.

**Definition 2** (Oblivious Set-member Decision Protocol): the user, Alice, inputs a private secret, $k$, and the server, Bob, inputs a private set, $\{k_1, k_2, \dots, k_n\}$. After executing this protocol, Alice outputs nothing but Bob outputs whether the secret $k$ belongs to the set of $\{k_1, k_2, \dots, k_n\}$. In addition, this protocol should satisfy:

**Correctness**: Bob gets 1 if $k$ is a member of the set of $\{k_1, k_2, \dots, k_n\}$ and 0 otherwise.

**Alice's Privacy**: Bob can not get any other secret information about the secret $k$ except knowing whether it is a member of the set of $\{k_1, k_2, \dots, k_n\}$.

**Alice's anonymity**: If $k$ is a member of the set of $\{k_1, k_2, \dots, k_n\}$, Bob should not know which member is equal to the secret, $k$. That is, he don't know the specific subscript, $i$, such that $k = k_i$ ($i \in \{1,2, \dots, n\}$).

**Bob's Privacy**: Alice can not know any secret information about the set of $\{k_1, k_2, \dots, k_n\}$.

### B. PROTOCOL

Suppose Alice's secrets $k$ and Bob's all $k_i s$ are the elements of the set of $\mathbb{Z}_N^* = \{1,2, \dots, N-1\}$. Now, let us describe the proposed OSMD protocol in detail as follows:

1) Bob first generates an $N$-element database (see FIG 1), where the $j$th element $p(j) = 1$ if $j = k_i$ ($i \in [1, n]$), and $p(j) = 0$ otherwise (encoding). Then Bob randomly generates $r_1, r_2, \cdots r_l \in \{0,1\}$ and further computes $q_t(j) = p(j) \oplus r_t$ for $t = 1$ to $l$ and $j = 1$ to $N-1$ (encrypting), where $l$ is a security parameter. Please note that Alice and Bob agree to let $p(0) = 0$ and $q_1(0) = q_2(0) = \cdots = q_l(0) = 0$ in advance.
2) Alice prepares $l$ log$N$-qubit registers, where one contains the encoded state $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$ ($k$ is Alice's secret), and the others contain $l-1$ decoy states: $\frac{|0\rangle+|j_1\rangle}{\sqrt{2}}$, $\frac{|0\rangle+|j_2\rangle}{\sqrt{2}}$, …, $\frac{|0\rangle+|j_{l-1}\rangle}{\sqrt{2}}$ (all $j_i$ s are random integers in $\mathbb{Z}_N^*$). Furthermore, Alice sends all $l$ registers to Bob in random order (as shown in FIG 2), and make a record of the order of the sent sequences.
3) After receiving all registers from Alice, Bob applies an oracle $O_t$ on the $t$th register for $t = 1$ to $l$ and then sends them back to Alice. Where the oracle is and works as follows [9]:

$$O_t = \begin{pmatrix} (-1)^{q_t(0)} & & \\ & \ddots & \\ & & (-1)^{q_t(N-1)} \end{pmatrix}, \quad (1)$$

$$|\psi_1\rangle = \frac{|0\rangle+|j\rangle}{\sqrt{2}} \xrightarrow{O_t} |\psi_2\rangle, \quad (2)$$

$$|\psi_2\rangle = \frac{|0\rangle+(-1)^{q_t(j)}|j\rangle}{\sqrt{2}}. \quad (3)$$

4) For each decoy state returned from Bob, Alice performs an honest test. That is, Alice check whether the superposition in the returned state was preserved as follows: $\frac{|0\rangle_{Q_i}+|j_i\rangle_{Q_i}}{\sqrt{2}}$ or $\frac{|0\rangle_{Q_i}-|j_i\rangle_{Q_i}}{\sqrt{2}}$, since the two possible states are obviously orthogonal and further she knows $j_i$. If Alice finds a cheat of Bob, she will terminate this protocol. Otherwise continue to the next step.
5) For the encoded state returned from Bob, Alice will perform the unitary operations as follows:

$$\prod_{t=1}^{\mathbb{I}} U_{cnot(1,\mathbb{I}_t)} U_{swap(1,\mathbb{I}_f)} \frac{|0\rangle \pm |k\rangle}{\sqrt{2}} = |\pm\rangle|0\rangle^{\otimes(m-1)}. \quad (4)$$

Where $m = \log N$ and there are $\mathbb{I}$ ones in the binary representation of $k$, with $\mathbb{I}_f$ pointing to the first "1" and $\mathbb{I}_t$ pointing to the $t$th "1". $U_{swap(1,\mathbb{I}_f)}$ is a unitary operation which swaps between the first and the $\mathbb{I}_f$th qubit. This operation ensures the first qubit is a one. In addition, $U_{cnot(1,\mathbb{I}_t)}$ is a $CNOT$ gate operation which the first qubit is the control qubit and the $\mathbb{I}_t$th qubit is a target qubit. After performing the above unitary operations, Alice measures only the first qubit in the encoded state on the basis of $\{|+\rangle, |-\rangle\}$. If she gets $|+\rangle$, then $q_s(k) = 0$, where $s$ is the order of the encoded state in the sent sequences. Otherwise, $q_s(k) = 1$.
6) Alice sends $q_s(k)$ and $s$ to Bob by the authenticated classical channel.
7) After receiving the classical information, $q_s(k)$ and $s$, Bob computes $p(k) = q_s(k) \oplus r_s$. If $p(k) = 1$, then he can decide that Alice's secret belongs to his private set (i.e. $k \in \{k_1, k_2, \dots, k_n\}$). Otherwise, $k \notin \{k_1, k_2, \dots, k_n\}$.

### C. ANALYSIS

Since the states of $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$ and $\frac{|0\rangle-|k\rangle}{\sqrt{2}}$ are obviously orthogonal, it is perfectly possible to distinguish between them by doing a Von Neumann measurement [7-9]. Furthermore, Alice can rightly get $q_s(k)$ by distinguishing the encoded state returned from Bob, and further Bob can privately obtain $p(k)$. That is, this protocol clearly and rightly works when Alice and Bob honestly execute the protocol.

On the one hand, Bob's privacy rests on his encrypting method, which is one-time pad. If Alice honestly executing this protocol, obviously she can only get $q_s(k)$, instead of $p(k)$. Since $q_s(k) = p(k) \oplus r_s$ and $r_s$ is unknown and random, so Alice can't know $p(k)$. Even if Alice is dishonest, she can get at most $l$ $q_t(j)$s. However, by these $q_t(j)$s, she can't still obtain any $p(j)$ rightly, because Bob uses one-time pad to encrypt $p(j)$ (that is, all $r_t$s are random and unknown). Therefore, Alice can't get any secret information about the private set of $\{k_1, k_2, \dots, k_n\}$ in the proposed protocol.

On the other hand, Alice's privacy depends on Bob's impossibility of distinguishing the encoded quantum state sent from Alice. Two basic elements of quantum theory enforce this: No-cloning Theorem which forbids the creation of identical copies of an arbitrary unknown quantum state, and Heisenberg Uncertainty Principle which implies that it is impossible to measure the state of any system without disturbing that system.

To illustrate it concretely, we consider that Bob is dishonest. For a dishonest Bob, it is possible to perform an intercept and resend attack. That is, when he receives the state of $\frac{|0\rangle+|j\rangle}{\sqrt{2}}$, he first measures it and then prepares and resends a new state by his measured results. Since he doesn't know $j$, he can't rightly perform a Von Neumann measurement to distinguish the received state. If he only applies a simple projective measurement, he might eventually succeed to pass the honest test, but not with the probability of more than $\frac{1}{2}$. In our protocol, however, Alice's secret state is sent in random order, that is, it is hided in other $l-1$ decoy states. So, if Bob wants to get Alice's secret by this attack, the success probability is not more than $2^{-l}$.

Furthermore, we discuss a more complicated entangle-measure attack by a dishonest Bob that he is able to prepare an ancillary system and entangle the ancillary system with the states transmitted from Alice to him by his local unitary operations, and afterwards he can measure the ancillary system to get the partial information about Alice's secret. For simplicity, we only consider the encoded state of $\frac{|0\rangle+|k\rangle}{\sqrt{2}}$. Suppose that the initial state of the ancillary system is $|0\rangle_B$ and Bob's dishonest action when he receives Alice's register can be described by a unitary operator $\widetilde{U}_{QB}$, which acts on the register $Q$ and the ancillary system $B$. We can describe it as follows:

$$\widetilde{U}_{QB}|0\rangle_Q|0\rangle_B = \sqrt{\eta_0}|0\rangle_Q|\phi_0\rangle_B + \sqrt{1-\eta_0}|V_0\rangle_{QB}, \quad (5)$$

$$\widetilde{U}_{QB}|k\rangle_Q|0\rangle_B = \sqrt{\eta_k}|k\rangle_Q|\phi_k\rangle_B + \sqrt{1-\eta_k}|V_k\rangle_{QB}, \quad (6)$$

$$\widetilde{U}_{QB}\left(\tfrac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_Q|0\rangle_B = \sqrt{\eta_{+k}}\left(\tfrac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_Q|\phi_{+k}\rangle_B + \sqrt{1-\eta_{+k}}|V_{+k}\rangle_{QB}, \quad (7)$$

where $|V_0\rangle_{QB}$, $|V_k\rangle_{QB}$ and $|V_{+k}\rangle_{QB}$ are a vector orthogonal to $|0\rangle_Q|\phi_0\rangle_B$, $|k\rangle_Q|\phi_k\rangle_B$ and $|+k\rangle_Q|\phi_{+k}\rangle_B$ ($|+k\rangle = \frac{|0\rangle+|k\rangle}{\sqrt{2}}$), respectively, i.e.,

$$ {}_Q\langle 0|_B\langle\phi_0|V_0\rangle_{QB} = 0, \quad (8)$$

$$ {}_Q\langle k|_B\langle\phi_k|V_k\rangle_{QB} = 0, \quad (9)$$

$$ {}_Q\langle +k|_B\langle\phi_{+k}|V_{+k}\rangle_{QB} = 0. \quad (10)$$

From Eqs. (5) and (6), we can easily deduce that the following equation holds:

$$\begin{aligned}\widetilde{U}_{QB}\left(\tfrac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_Q|0\rangle_B &= \frac{1}{\sqrt{2}}(\widetilde{U}_{QB}|0\rangle_Q|0\rangle_B + \widetilde{U}_{QB}|k\rangle_Q|0\rangle_B) \\ &= \frac{1}{\sqrt{2}}(\sqrt{\eta_0}|0\rangle_Q|\phi_0\rangle_B + \sqrt{1-\eta_0}|V_0\rangle_{QB} \\ &\quad + \sqrt{\eta_k}|k\rangle_Q|\phi_k\rangle_B + \sqrt{1-\eta_k}|V_k\rangle_{QB}). \quad (11)\end{aligned}$$

If we compute the scalar product between Eqs. (7) and (11), we will obtain the identity

$$\begin{aligned}1 = {} & \tfrac{\sqrt{\eta_0\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_0\rangle_B + \tfrac{\sqrt{\eta_0(1-\eta_{+k})}}{\sqrt{2}}\,{}_{QB}\langle V_{+k}|0\rangle_Q|\phi_0\rangle_B \\ & + \tfrac{\sqrt{(1-\eta_0)\eta_{+k}}}{\sqrt{2}}\,{}_Q\langle +k|_B\langle\phi_{+k}|V_0\rangle_{QB} + \\ & \tfrac{\sqrt{(1-\eta_0)(1-\eta_{+k})}}{\sqrt{2}}\,{}_{QB}\langle V_{+k}|V_0\rangle_{QB} + \\ & \tfrac{\sqrt{\eta_k\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_k\rangle_B + \\ & \tfrac{\sqrt{\eta_k(1-\eta_{+k})}}{\sqrt{2}}\,{}_{QB}\langle V_{+k}|k\rangle_Q|\phi_k\rangle_B + \\ & \tfrac{\sqrt{(1-\eta_k)\eta_{+k}}}{\sqrt{2}}\,{}_Q\langle +k|_B\langle\phi_{+k}|V_k\rangle_{QB} + \\ & \tfrac{\sqrt{(1-\eta_k)(1-\eta_{+k})}}{\sqrt{2}}\,{}_{QB}\langle V_{+k}|V_k\rangle_{QB}\,. \quad (12)\end{aligned}$$

Then we get

$$1 < \frac{\sqrt{\eta_0\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_0\rangle_B + \frac{\sqrt{\eta_0(1-\eta_{+k})}}{\sqrt{2}} + \frac{\sqrt{(1-\eta_0)\eta_{+k}}}{\sqrt{2}} + \frac{\sqrt{(1-\eta_0)(1-\eta_{+k})}}{\sqrt{2}} + \frac{\sqrt{\eta_k\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_k\rangle_B + \frac{\sqrt{\eta_k(1-\eta_{+k})}}{\sqrt{2}} + \frac{\sqrt{(1-\eta_k)\eta_{+k}}}{\sqrt{2}} + \frac{\sqrt{(1-\eta_k)(1-\eta_{+k})}}{\sqrt{2}}. \quad (13)$$

Suppose that the probability of Bob's passing the honest test is higher than a certain threshold, i.e.,

$$\eta_0 > 1-\varepsilon,\quad \eta_k > 1-\varepsilon,\quad \eta_{+k} > 1-\varepsilon. \quad (14)$$

By Eqs.(13) and (14), it gives

$$1 < \frac{\sqrt{\eta_0\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_0\rangle_B + \frac{\sqrt{\eta_k\eta_{+k}}}{2}\,{}_B\langle\phi_{+k}|\phi_k\rangle_B + 2\sqrt{2}\sqrt{\varepsilon} + \sqrt{2}\varepsilon. \quad (15)$$

It implies the following conditions hold,

$${}_B\langle\phi_{+k}|\phi_0\rangle_B > 1 - 2(\sqrt{2} + \tfrac{\sqrt{\varepsilon}}{\sqrt{2}})\sqrt{\varepsilon}, \quad (16)$$

$${}_B\langle\phi_{+k}|\phi_k\rangle_B > 1 - 2(\sqrt{2} + \tfrac{\sqrt{\varepsilon}}{\sqrt{2}})\sqrt{\varepsilon}. \quad (17)$$

From Eqs. (16) and (17), it shows that if $\varepsilon \to 0$, then ${}_B\langle\phi_{+k}|\phi_0\rangle_B \to 1$ and ${}_B\langle\phi_{+k}|\phi_k\rangle_B \to 1$. That is, if Bob wants to be sure that he fully passes the honest test, then the final states of the ancillary system $B$ for any choice of $k$ will coincide with $|\phi_0\rangle_B$, that is, the states of the ancillary system $B$ are independent of the secret $k$.

Furthermore, we give an upper bound to Bob's information on the secret $k$ by considering the mutual information $I$ that connects the classical variable $k \in \{1,2,\dots,N-1\}$, which labels Alice's secret, and Bob's estimation of this variable. The ancillary system $B$ can be characterized by the quantum ensemble $\mathcal{E} \equiv \{p_k = \frac{1}{N}, \rho_B(k)\}$ [8], where $p_k = \frac{1}{N}$ is Alice's probability of owning the secret $k$ (Assuming that initially Bob does not have any prior information on the value of $k$), and

$$\rho_B(k) = Tr_Q(|\Psi\rangle_{QB}\langle\Psi|) = \eta_{+k}\sigma_k + (1-\eta_{+k})\tilde{\sigma}_k, \quad (18)$$

with

$$|\Psi\rangle_{QB} = \widetilde{U}_{QB}\left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_Q|0\rangle_B = \sqrt{\eta_{+k}}\left(\frac{|0\rangle+|k\rangle}{\sqrt{2}}\right)_Q|\phi_{+k}\rangle_B + \sqrt{1-\eta_{+k}}|V_{+k}\rangle_{QB},$$
$$\sigma_k = |\phi_{+k}\rangle_B\langle\phi_{+k}|. \quad (19)$$

From the Holevo bound [18], we obtain

$$I \le \mathcal{X}(\mathcal{E}) = S(\rho_B) - \tfrac{1}{N}\textstyle\sum_{k=0}^{N-1} S(\rho_B(k)), \quad (20)$$

where $\rho_B = \sum_{k=0}^{N-1}\rho_B(k)/N$ is the average state of $B$. This allows us to write also

$$\rho_B = \eta\sigma + (1-\eta)\tilde{\sigma}, \quad (21)$$

with

$$\sigma \equiv \textstyle\sum_{k=0}^{N-1}\frac{\eta_{+k}}{N\eta}\sigma_k,\ \tilde{\sigma} \equiv \sum_{k=0}^{N-1}\frac{1-\eta_{+k}}{N(1-\eta)}\tilde{\sigma}_k, \quad (22)$$

where $\eta = \sum_k \eta_{+k}/N$ is Bob's average probability of passing the honest test, which must be greater than $1-\varepsilon$. Equations (18) and (21) can then be exploited to produce the following inequalities [8]

$$S(\rho_B) \le H_2(\eta) + \eta S(\sigma) + (1-\eta)S(\tilde{\sigma}), \quad (23)$$

$$S(\rho_B(k)) \ge \eta_{+k}S(\sigma_k) + (1-\eta_{+k})S(\tilde{\sigma}_k), \quad (24)$$

where $H_2(x) \equiv -x\log x - (1-x)\log(1-x)$ is the binary entropy. Therefore Eq. (20) gives

$$I \le H_2(\eta) + \eta\mathcal{X}\left(\left\{\frac{\eta_{+k}}{N\eta};\sigma_k\right\}\right) + (1-\eta)\mathcal{X}\left(\left\{\frac{1-\eta_{+k}}{N(1-\eta)};\tilde{\sigma}_k\right\}\right), \quad (25)$$

where $\mathcal{X}\left(\left\{\frac{1-\eta_{+k}}{N(1-\eta)};\tilde{\sigma}_k\right\}\right)$ is the Holevo information associated with a source characterized by probabilities $\frac{1-\eta_{+k}}{N(1-\eta)}$. This quantity can never be bigger than $\log_2 N$ (the same applies to $\mathcal{X}\left(\left\{\frac{\eta_{+k}}{N\eta};\sigma_k\right\}\right)$, but we are not going to use it). Therefore, we can write

$$I \le H_2(\eta) + \eta\mathcal{X}\left(\left\{\frac{\eta_{+k}}{N\eta};\sigma_k\right\}\right) + (1-\eta)\log_2 N. \quad (26)$$

By Eq. (16), the density matrices $\sigma_k$ can be decomposed as the following expression

$$\sigma_k = q_k|\phi_0\rangle\langle\phi_0| + (1-q_k)\tau_k + \Delta_k, \quad (27)$$

where $\tau_k$ are density matrices formed by vectors $|v_\perp\rangle$ orthogonal to $|\phi_0\rangle$, $\Delta_k$ are traceless operators containing off-diagonal terms of the form $|\phi_0\rangle\langle v_\perp|$, and the probabilities satisfy the following conditions

$$q_k = \langle\phi_0|\sigma_k|\phi_0\rangle = \langle\phi_0|\phi_{+k}\rangle\langle\phi_{+k}|\phi_0\rangle > 1 - 8\sqrt{\varepsilon}. \quad (28)$$

Accordingly, we can write also

$$\sigma = q|\phi_0\rangle\langle\phi_0| + (1-q)\tau + \Delta, \quad (29)$$

$$q = \langle\phi_0|\sigma|\phi_0\rangle = \textstyle\sum_{k=0}^{N-1}\frac{\eta_{+k}}{N\eta}q_k > 1 - 8\sqrt{\varepsilon}. \quad (30)$$

Therefore, we can get

$$\mathcal{X}\left(\left\{\frac{\eta_{+k}}{N\eta};\sigma_k\right\}\right) \le S(\sigma) \le S(q|\phi_0\rangle\langle\phi_0| + (1-q)\tau) \le H_2(q) + (1-q)S(\tau) \le H_2(q) + (1-q)\log_2 N. \quad (31)$$

Replacing this into Eq. (26), we finally obtain

$$I \le H_2(\eta) + \eta H_2(q) + (1-\eta q)\log_2 N. \quad (32)$$

It implies (by Eq. (30))

$$I \le c\sqrt{\varepsilon}\log_2 N. \quad (33)$$

This means that Alice can limit Bob's information $I$, by employing in her tests a value of $\varepsilon$ sufficiently small. In turn, if Bob wants to pass the honest test with high

probability, he must retain low information on Alice's secret.

In addition, Alice's anonymity is based on her privacy, which ensures that Bob honestly executes the protocol. On the one hand, obviously Bob can't directly measure the received quantum states to get Alice's secret information. Otherwise he will not completely pass the honest test. On the other hand, he can't yet obtain any correlation between Alice's secret and his certain member, only by the received classical information ( $q_s(k)$ and $s$ ). Therefore, the proposed protocol guarantees Alice's anonymity.

Finally, we evaluate communication costs of the proposed protocol. As shown in FIG 2 and FIG 3, we can easily see that the numbers of the exchanged quantum and classical messages are $2l$ and 2, respectively, which are all independent of the number of the elements of the set, $n$, so the communication complexity is constant, $O(1)$.

## III. CONCLUSION

In this paper, we presented and defined the Oblivious Set-member Decision problem and then proposed a quantum protocol to solve this problem. In the proposed protocol, the server first creates a private database by the private set and then introduces an oracle to perform the phase transformation on the encoded state, so that he can finally know whether the user's secret belongs to his private set in an oblivious manner. In turn, the user utilizes the decoy technology to prevent the dishonesty of the server. Especially, the communication complexity of the proposed protocol is reduced to the constant, $O(1)$ , instead of $O(n)$ . Therefore, the proposed protocol is especially suitable for oblivious set-member decision of the large-size set or dataset.

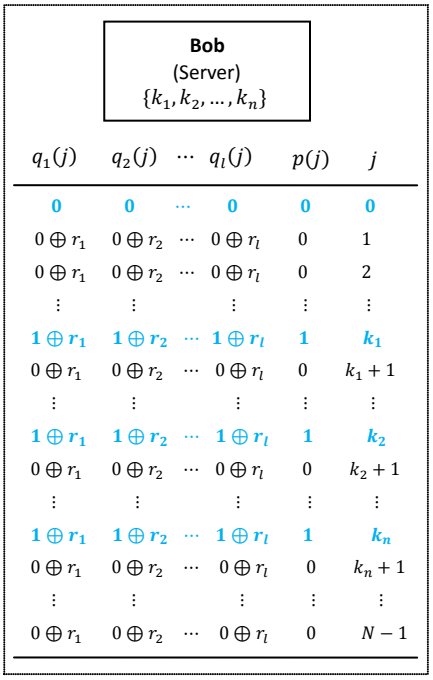
Like most classical/quantum secure multi-party protocols, it can use classical/quantum bit commitment, zero-knowledge proof and other verifiable technologies to ensure that the parties honestly execute the protocol. This is our future work.

## ACKNOWLEDGMENTS

This work was supported by National Natural Science Foundation of China (61173187, 61173188 and 11301002), the Ministry of Education institution of higher learning doctor discipline and scientific research fund aids a project financially (20133401110004), Natural Science Foundation of Anhui Province (1408085QF107), and the 211 Project of Anhui University (33190187 and 17110099).

## References

[1] P. Arrighi, and L. Salvail, Int. J. Quant. Inf. 4 p.883 (2006).
[2] A. Broadbent, J. Fitzsimons, E. Kashefi, in Proc. 50th Annual IEEE Symposium of Foundations of Computer Science, Atlanta, GA, 2009, p.517.
[3] T. Morimae, K. Fujii, Phys. Rev. A 87 050301 (2013)
[4] V. Giovannetti, L. Maccone, T. Morimae, and T.G. Rudolph, Phys. Rev. Lett. 111 230501 (2013).
[5] T. Morimae, Phys. Rev. A 89 060302 (2014).
[6] M. Liang, Quantum Inf. Process. 12 p.3675 (2013).
[7] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. 100 230502 (2008).
[8] V. Giovannetti, S. Lloyd, and L. Maccone, IEEE T. Inform. Theory 56, 3465 (2010).
[9] L. Olejnik, Phys. Rev. A 84 022313 (2011).
[10] M. Jakobi, C. Simon, N. Gisin, et al., Phys. Rev. A 83 022301 (2011).
[11] A. Mandilara, N.J. Cerf, Phys. Rev. A 85 062310 (2012).
[12] A. Kent, Phys. Rev. Lett. 109 130501 (2012).
[13] G.P. He, Quantum Inf. Process. 13 p.2195 (2014).
[14] R. Loura, A.J. Almeida, P.S. Andre, et al., Phys. Rev. A 89 052336 (2014).
[15] S. Winkler, J. Wullschleger, in Proc. 30th Annual International Cryptology Conference Santa Barbara, Ca, 2010, p.707.
[16] J. Sikora, Quantum Inf. Comput. 12 p.609 (2012).
[17] A. Chailloux, I. Kerenidis, and J. Sikora, Quantum Inf. Comput. 13 p.158 (2013).
[18] A. Holevo, Probabilistic and Statistical Aspects of Quantum Theory (Publications of the Scuola Normale Superiore, Springer, 2011).




| $q_1(j)$ | $q_2(j)$ | $\cdots$ | $q_l(j)$ | $p(j)$ | $j$ |
|---|---|---|---|---|---|
| **0** | **0** | $\cdots$ | **0** | **0** | **0** |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | 1 |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | 2 |
| $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathbf{1 \oplus r_1}$ | $\mathbf{1 \oplus r_2}$ | $\cdots$ | $\mathbf{1 \oplus r_l}$ | **1** | $\boldsymbol{k_1}$ |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | $k_1 + 1$ |
| $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathbf{1 \oplus r_1}$ | $\mathbf{1 \oplus r_2}$ | $\cdots$ | $\mathbf{1 \oplus r_l}$ | **1** | $\boldsymbol{k_2}$ |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | $k_2 + 1$ |
| $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\vdots$ |
| $\mathbf{1 \oplus r_1}$ | $\mathbf{1 \oplus r_2}$ | $\cdots$ | $\mathbf{1 \oplus r_l}$ | **1** | $\boldsymbol{k_n}$ |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | $k_n + 1$ |
| $\vdots$ | $\vdots$ | | $\vdots$ | $\vdots$ | $\vdots$ |
| $0 \oplus r_1$ | $0 \oplus r_2$ | $\cdots$ | $0 \oplus r_l$ | 0 | $N - 1$ |

**FIG 1. The *N*-element database created by the private set of $\{\boldsymbol{k_1}, \boldsymbol{k_2}, \dots, \boldsymbol{k_n}\}$.**

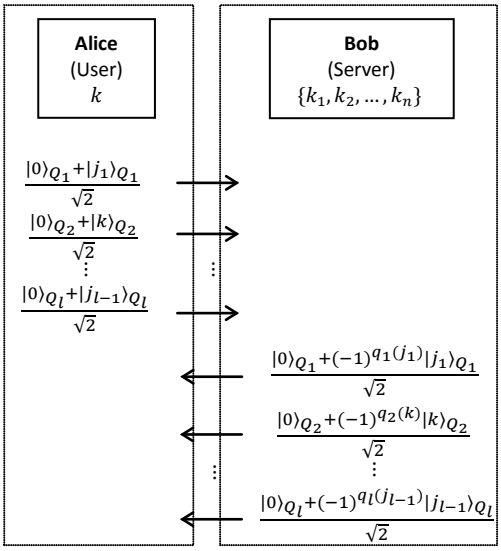



**FIG 2. The exchanged quantum information between Alice and Bob.**

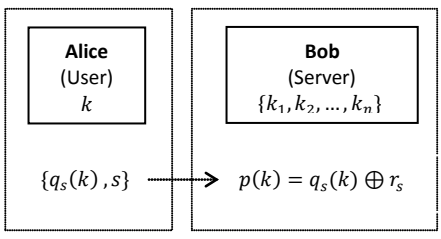



**FIG 3. The exchanged classical information between Alice and Bob.**